Department of the Army
Pamphlet 340–6

Office Management

Defense Privacy Board Decision Memoranda

Headquarters
Department of the Army
Washington, DC
15 October 1983

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 340–6
Defense Privacy Board Decision Memoranda

This Change 1--

- Replaces paragraph 14, DoD Decision No. 14, which is superseded by a new decision, entitled 'Release of Information for Purposes of Commercial Solicitation.'

- Reflects this change in both the table of contents and the index.

- This Army pamphlet--

- Contains guidelines on a wide range of privacy issues presented to the Defense Privacy Board for resolution or clarification. They were issued as Defense Privacy Board Decision Memoranda 76-1, 76-2, 77-1, 78-1, 80-1, 82-1, and 82-2; but are combined in the pamphlet, with an index, for ease of referral and use as a reference document.

Headquarters
Department of the Army
Washington, DC
15 October 1983

Department of the Army Pamphlet 340–6

Office Management

Defense Privacy Board Decision Memoranda

By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR
General, United States Army
Chief of Staff

Official:

ROBERT M. JOYCE
Major General, United States Army
The Adjutant General

History. This publication was originally printed on 1 May 1983. It was authenticated by E. C. Meyer, Chief of Staff and Robert M. Joyce, The Adjutant General. This electronic edition publishes the basic 1 May 1983 edition and incorporates Change 1. Change 1 to this regulation was printed on 15 October 1983. Change 1 was authenticated by John A. Wickham, Jr., Chief of Staff and Robert M. Joyce, The Adjutant General.

Summary. Not Applicable.

Applicability. Not Applicable.

Proponent and exception authority. The proponent agency of this pamphlet is the US Army Adjutant General Center.

Interim changes. Interim changes are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration date unless sooner superseded or rescinded.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) direct to HQDA(DAAG-AMR-S), Alexandria, VA 22331.

Distribution. *Active Army, ARNG, USAR:* To be distributed in accordance with DA Form 12-9A requirements for Office Management—D.

Contents (Listed by paragraph and page number)

UNCLASSIFIED

Contents—Continued

Contents—Continued

RESERVED

1. PROVIDING WAGE AND EARNING STATEMENTS (W-2 FORMS) FOR MILITARY PERSONNEL TO STATE AND LOCAL TAX AUTHORITIES

The question presented is whether the Privacy Act permits the dissemination of wage and earning information W-2 Forms to state, local, and other taxing authorities. The information contained on W-29 Forms pertaining to members and employees is required to be disclosed to state and local taxing authorities under the Freedom of Information Act, 5 U.S.C. 552. No accounting of such disclosures is required. To the extent that the dissemination of such data could be considered an invasion of personal privacy, on the balance, any potential harm which, may be suffered by a military member is far outweighed by the public interest in the dissemination of such data.

2. APPLICABILITY TO DECEASED PERSONS

The question presented is whether the Privacy Act of 1974 (5 U.S.C. 552a) prohibits the release of personal information concerning deceased service members or employees. Examples of such data include dates of service, date and place of birth, date and geographical location of death, cause of death, place of burial, and service number.

The Privacy Act, as interpreted in the OMB guidelines, does not protect the records of deceased individuals from disclosure (see 40 FR 28951, July 9, 1975). Generally, in the case of decedents, personal information may be disclosed. The Freedom of Information Act (5 U.S.C. 552a), however, authorizes withholding of some data to protect the privacy of relatives of the decedent—see DoD 5400.7–R, paragraph 3–200, No. 6b.

3. DISCLOSURE OF PERSONAL RECORDS OF PERSONS MISSING IN ACTION OR OTHERWISE UNACCOUNTED FOR. CONTAINED IN A SYSTEM OF RECORDS, TO THEIR NEXT-OF-KIN

The question presented is what personal information relating to persons missing in action or otherwise unaccounted for may be disclosed under the Privacy Act of 1974 (5 U.S.C. 552a).

In the event a legal guardian has been appointed by a court of competent jurisdiction for a member who is missing in action or otherwise unaccounted for then the guardian would be in the position, of the member and have the same rights of access to records as the member would have. *See* 5 U.S.C. 552a(h). If a guardian has been appointed, personal records which are contained in a system of records and relate to the missing member should not be disclosed to other persons without written consent of the guardian unless disclosure is authorized by 5 U.S.C. 552a(b).

Personal information relating to persons missing in action or otherwise unaccounted for must be disclosed "pursuant to the Order of a court of competent jurisdiction." 5 U.S.C. §551a(b)(11); *see Stiles v. Atlanta Gas Light Co.*, 453 F. Supp. 798, 800 (N.D. Ga. 1978) (court must specifically direct disclosure for compelling reasons). In a case involving the families of military personnel missing in action, one court ordered, in part, that next-of-kin receiving governmental financial benefits, which could be terminated by a status review be afforded "reasonable access to the information upon which the status review will be based." *McDonald v. McLucas*, 371 F. Supp. 831, 836 (S.D.N.Y.); *affd mem.*, 419 U.S. 987 (1974).

Since a status review is likely to require access to almost all of the significant information in a system of records pertaining to a member who is missing in action. This order would appear to constitute sufficient authority under the Privacy Act for disclosure of almost any personal records of interest.

Any information in a system of personal records not coming within the ambit of the court order may be made available to the next-of-kin under the Freedom of Information Act. If release of the records concerned does not constitute a clearly unwarranted invasion of personal privacy (5 U.S.C. §552(b)(6)). In determining what information must be disclosed under this standard, a balancing test which weighs, the public interest in disclosure against the potential invasion of personal privacy should be conducted. *See* DoD 5400.7-R, paragraph 3-200, No. 6; *see e.g., Department of the Air Force v. Rose*, 425 U.S. 352 (1976); *Church of Scientology v. U.S. Department of Defense*, 611 F.2d 738, 746 (9th Cir. 1979) (four factors to be weighed).

Because the facts and needs will differ in each case, the balancing test may require disclosure of information in one circumstance but its denial in another circumstance. *See Getman v. NLRB*, 450 F.2d 670 (D.C. Cir. 1971), app'l for stay of order denied, 404 US 1204 (1971); *Robles v. Environmental Protection Agency*, 484 F.2d 843 (4th Cir. 1973); *Wine Hobby, USA, Inc. v. United States Bureau of Alcohol, Tobacco and Firearms*, 502 F.2d 133 (3rd Cir. 1974).

Due to the unusual circumstances involved when a service member is missing in action or otherwise unaccounted for, his or her next-of-kin may have a more compelling case for release of a requested record than would other third parties. However, each such request must be evaluated on its own merits.

4. CORRECTIONS OF MILITARY RECORDS PERMITTED UNDER THE ACT

This addresses the question of when requests for correction of records should be processed under the Privacy Act of

1974 (5 U.S.C. 552a) and when an individual must seek correction by the Boards for Correction of Military and Naval Records. The question presented is whether the Privacy Act amendment provision (5 U.S.C. 552a(d)(2)) permits an individual to request corrections of all errors he or she believes to exist in his or her records, that are maintained in a system of records. One of the main purposes of the Privacy Act was to insure that personal records relating to individuals are maintained accurately so that informed decisions based upon those records could be made. The Privacy Act amendment provision permits an individual to request factual amendments to his or her records. It does not ordinarily permit correction of judgmental decisions such as efficiency reports or selection and promotion board reports. These judgmental decisions should be challenged before the Boards for the Correction of Military and Naval Records which by statute, 10 U.S.C. 1552, are authorized to make these determinations. While factual amendments may be sought under both the Privacy Act and the procedures of the Boards for Correction of Military and Naval Records. Attempts to correct other than factual matters ordinarily fall outside of the provisions of the Privacy Act and fall within the purview of the Boards for Correction of Military and Naval Records. If a factual matter is corrected under Privacy Act procedures, any subsequent judgmental decisions that may have been affected by the factual correction, if contested, should be considered by the Boards for the Correction of Military and Naval Records.

5. APPLICABILITY TO NATIONAL GUARD RECORDS

The question presented is whether the Privacy Act applies to records maintained by the National Guard. As used in the Privacy Act. "maintain" connotes the various records keeping functions to which the Act applies, i.e., maintaining, collecting, using, and disseminating as well as control over and hence the responsibility and accountability for systems of records (OMB Cir. No. A-108, 40 FR 28948, 28954 (1975)).

Section 275, title 10, United States Code, requires that each armed force maintain personnel records on each member of its RESERVE COMPONENT. The RESERVE COMPONENTS of the Army and the Air Force includes the Army and Air National Guards of the United States respectively (10 U.S.C. 261) which are composed of federally recognized units and organizations of the Army or Air National Guard and members of the Army or Air National Guard who are also Reserves of the Army or Air Force respectively (10 U.S.C. 3077 and 8077). The mandate of section 275, title 10, United States Code requires the Departments of the Army and the Air Force to maintain personnel records on all members of the federally recognized units. And organizations of the Army and Air National Guards and on all members of the Army or Air National Guards who are also reserves of the Army and Air Force and are "maintained" by the Army or Air Force for the purpose of the Privacy Act. It is noted that these records are not all located at the National Guard Bureau. Some are located at the state and physically maintained by the state adjutant general. It is not, however, necessary that the records be physically located in the agency for them to be maintained by the agency (see OMB Cir. No. A-108, supra). The records located at the state level are under the direct control of the Army or Air Force in that they are maintained by the state as prescribed by regulations (NGR 600-200 and AFR 35-44) which implement section 275, title 10, United States Code, and are promulgated pursuant to the authority of the Secretaries of the Army and the Air Force (10 U.S.C. 280). These records are, therefore, Army or Air Force records and subject to the provisions of the Privacy Act.

The determination that these records are subject to the Privacy Act does not mean that they cannot be used by the members of the state national guards unless such use is listed as a routine use and an accounting is kept. The state officials who use and maintain these records are members of the reserves (members of the Army or Air Force National Guard of the United States), And disclosure to them for the performance of their duties is a disclosure within the Department of Defense which, does not require a routine use or an accounting.

6. FEE ASSESSMENT TO CONGRESSMEN FOR RECORDS FURNISHED WHICH ARE SUBJECT TO THE PRIVACY ACT

The question presented is whether members of Congress should be charged for records provided at their request under the guidance contained in DoD Directive 5400.11. Section (f)(5) of the Privacy Act states that each agency shall "establish fees to be charged, if any, to any individual for making copies of his records. . .". OMB guidance and DoD Directive 5400.11 both point out that if a fee is charged, only the direct cost of making the copy may be collected. This guidance also states that if copying is the only means whereby the record can be made available to the individual, reproduction fees will not be assessed.

Therefore, the charging of a fee is a discretionary matter on the part of the agency. In view of this, it is proposed that from a policy standpoint, DoD not charge Congressmen for records furnished when requested under the Privacy Act, unless the charge would be substantial. In no event should a fee below $25.00 be determined substantial. It is recommended that in constituent inquiries where the fee is substantial, a suggestion should be made that the Congressman advise his constituent that the information may be obtained by writing the appropriate office and payment of the cost of reproduction. Additionally, the record may be examined at no cost if the constituent wishes to visit the custodian of the record.

7. RELEASE OF HOME OF RECORD TO MEMBERS OF CONGRESS

The question presented is the propriety under the Privacy Act of 1974 (5 U.S.C. 552a), of releasing a service member's "home of record" from his service record to an inquiring Member of Congress or Congressional staff member. The new routine use provisions for DoD Systems of Records published on 9 October 19-15 (40 FR 47748) which became effective on 8 November 1975 are sufficiently broad to permit the release of home of record information to a Member of Congress or Congressional staff member who is making an inquiry of a DoD Component at the request of the subject service member even if the subject member's request did not concern that particular portion of the service record.

It should be noted, however, that the service record entry for home of record is intended only to reflect the service member's home at the time of entry into the service or call to active duty. It may not reflect the member's current legal residence or domicile for voting purposes, and the Member of Congress or Congressional staff member may be more interested in the subject service member's legal residence as entered on a W-4 form by the service member and as reflected by the member's pay record. Any release of home of record information to a Member of Congress or to a Congressional staff member should be caveated with the notation that it only reflects the home address at the time of entry into the service or call to active duty.

8. DISCLOSURE ACCOUNTING FOR RECORDS DISCLOSED THROUGH MILITARY LEGISLATIVE LIAISON CHANNELS

The question presented is what procedures and divisions of responsibility should be established by military departments to ensure the preparation of required disclosure accountings where information concerning individuals is disclosed to Members of Congress through departmental legislative liaison channels from records maintained by other activities, with the consent of the individuals concerned, pursuant to the newly effective DoD "routine use." It is noted that, under subsection (c) of the Privacy Act of 1974 (5 U.S.C. 552a), disclosure accountings apparently are required in instances of consensual disclosures and disclosures made pursuant to subsection (b)(3).

Where a disclosure is made directly to a Member of Congress by an activity having custody of the record that is disclosed, no substantial question exists under present DoD policy as to that activity's responsibility for maintaining an appropriate record of the disclosure for future accounting purposes in accordance with that activity's procedures implementing the Privacy Act. A more difficult administrative problem arises, however, where the requested information is transmitted by the custodial activity to the legislative liaison activity for retransmittal—possibly in a form that deletes some data furnished by the custodial activity, or that consolidates the information with information from records in the custody of other activities—to the requesting Member of Congress. In the latter situation, it might frequently be impossible for the custodial activity to discharge the system manager's responsibility of compiling and maintaining an accurate record of what was actually disclosed to the requesting Congressional office unless the custodial activity receives feedback from the legislative liaison.

It is questionable whether an attempt should be made to resolve the problem on a DoD-wide scale, because the formulation of specific procedures and responsibilities in connection with maintaining records required for disclosure accounting purposes apparently will involve consideration of a number of factors which will vary among the different military departments and other DoD Components, such as internal organizational relationships, a Component's prescribed methods and responsibilities for responding to Congressional inquiries and possibly the characteristics of the particular records and record systems involved.

It is recommended that the liaison activity prepare a disclosure accounting to be maintained by the custodial activity. In each case where information is disclosed as a routine use, a record of disclosure should be made and maintained for five years or the life of the record, whichever is longer. Therefore, the disclosure of the information should make a record of disclosure which contains, as a minimum, the name, rank, grade or rating, social security number of the person from whose record disclosure is made; the date, nature and purpose of the disclosure; and the name of the person to whom the disclosure is made, and the Member of Congress for whom he works. The name, rank, grade or rating, duty station, and where applicable, office title of the person making the disclosure should also be included. This record of disclosure should then be forwarded to the person who maintains the record from which the disclosure is made, or such activity as is designated by competent authority.

9. DEFINITION OF A "MINOR"

The question presented is who is a "minor" for purposes of the Privacy Act. The Privacy Act provides that the parent of any minor may act on behalf of that individual. OMB guidelines stress that this provision is in the alternative and permissive and thereby not construed as limiting the minor's right to access.

Under common law, a minor is a male or female child under 21. This definition is generally accepted unless modified by state law or unless the minor is emancipated by agreement between the parent and child, by enlistment in the

military, by marriage, or by court order. In the view of the Privacy Board, the determination of minority would normally be dependent upon the state law where the minor is located. Determination therefore must be made on a case by case basis. In making these determinations, close attention should be given to the growing body of law allowing minors to make medical decisions about themselves without parental consent and the implied or express right of privacy of the minor contained therein.

Members of the armed forces are considered emancipated for purposes of the Privacy Act.

10. THE USE OF INFORMATION FROM CONFIDENTIAL SOURCES BY INVESTIGATIVE ACTIVITIES IN RELATION TO OMB GUIDELINES

The question presented is whether the OMB guidance on section (k)(2) of the Privacy Act requires disclosure of a confidential source if the individual concerned was denied a right, benefit or privilege as a result of the information received. Normally, investigative activities will list interviewees, companies, firms or agencies as confidential sources in reports of investigation when the releaser of the information specifically requests confidentiality as a condition precedent to providing the information.

Subsection (k)(2) of the Office of Management and Budget (OMB) Privacy Act Implementation Guidelines states, in part, the following concerning confidential source information:

"Furthermore, the acceptance of this section in no way precludes an individual from knowing the *substance and source* of confidential information, should that information be used to deny him a promotion in a government job, or access to classified information or some other right, benefit, or privilege for which he was entitled to bring legal action when the government wished to base any part of its legal case on that information." (emphasis supplied)

Investigative activities are concerned about the possibility of an individual requestor taking adverse action based upon confidential *source* information in the report of investigation which could result in having to divulge the identity of the confidential source.

That portion of the quoted OMB language relating to an individual ". . . knowing the substance and source of confidential information . . . " appears to be in direct conflict with all of the preceding language of subsection (k)(2) of the guidelines, which provides very clearly for withholding the identity of a source in a proper case. OMB was queried concerning this apparent conflict and advised that the quoted section of Senator Ervin's statement relates not to the *administrative* process of declining to identify a source pursuant to subsection (k)(2) of the Act, but to the requestor's *judicial* remedies afforded by the Discovery Rules and subsection (g)(3)(A) of the Act.

In view of the foregoing, no objection is perceived as to the current administrative procedures of investigative activities of utilizing confidential sources in reports of investigations, which appear to be consistent with the Privacy Act and the OMB guidelines.

11. APPLICATION OF ACT TO INFORMATION FROM HOSPITAL COMMITTEE

The question presented is whether hospital committee minutes must be provided to patients or physicians under the Privacy Act. Hospital committee minutes such as medical audit, tissue, utilization, medical records and credentials, are not filed and indexed under the name or identifying number of the patient or physician. These minutes are not systems of records which are subject to the requirements of the Privacy Act. Therefore, access to these minutes need not be granted to the patient/physician under the Privacy Act.

12. ACCOUNTING FOR MASS DISCLOSURES OF PERSONAL INFORMATION TO OTHER AGENCIES

The question presented is whether interagency support agreements could be negotiated which would negate the requirement to account where "mass" disclosures are made to other specific agencies such as GAO. 5 U.S.C. 552a(c) requires that, except for intra-agency disclosures made pursuant to the Freedom of Information Act (FOIA), each agency keep an accurate accounting of all disclosures made from systems of records under its control. Generally, mass disclosures made to other government agencies fall under this requirement and an accounting is required.

Neither the Act nor OMB guidelines, however, specify a form for maintaining this accounting. They require only that an accounting be maintained, that the accounting be available to the individual named in the record and for use to advise of corrections of records and that it be maintained in such a way that a disclosure of records may be traced to the records disclosed. Specific records need not be marked to reflect disclosure unless necessary to satisfy this tracing requirement.

Accordingly, with respect to mass disclosure, if the disclosure is of all records or all of a category of records or of records released at the request of the individuals, e.g., with transmittal of payroll checks to banks, it should be

satisfactory simply to identify the category of records disclosed including the other information required under 5 U.S.C. 552a(c) on some comprehensible form and make that form available, as necessary, to satisfy the accounting of disclosure provisions of the Act. Similarly, if the disclosures occur at fixed intervals, a statement, to this effect, as opposed to a statement at each occasion of release, should satisfy the accounting requirement. If the mass disclosure is not of a complete category of records but, for example, a random selection within a category, then the above information with a list of the individuals' records disclosed could be maintained. Appropriate officials could then review this list, as necessary, to provide information to satisfy the accounting provisions of the Act.

It is not deemed appropriate to enter into inter-support agreements with the General Accounting Office (GAO) since they are not an executive agency and the requirement to account for disclosure to GAO is specifically provided for in the Privacy Act. However, inter-agency support agreements may be entered with other executive agencies as specified in DoD Directive 4000.19 and authorized by the OMB guidelines.

13. RELEASE OF PERSONAL INFORMATION TO STATE AGENCIES TO VALIDATE UNEMPLOYMENT COMPENSATION CLAIMS OF FORMER FEDERAL EMPLOYEES AND MILITARY MEMBERS

The question presented is the propriety under the Privacy Act of 1974 (5 U.S.C. 552a) of releasing information from employment or service records as required by 5 U.S.C. 8506 and 8523 to State agencies administering unemployment compensation claims, The latter two sections require Federal agencies, under specified circumstances, to provide to appropriate State agencies personal information, including the period of Federal or military service, if any, the pay grade or amount of Federal wages and allowances, the reasons for termination of Federal service or discharge from military service, and the conditions under which a military discharge or resignation occurred.

Portions of the required information normally may be released to any requestor pursuant to the Freedom of Information Act and 5 U.S.C. 552a(b)(2), these include the period of Federal employment or military service, pay grade, wages and allowances received. Normally information concerning the reasons for termination or discharge and the conditions of discharge can only be released pursuant to the advance written consent of the subject individual provided by the State agency, 5 U.S.C. 552a(b), or under a routine use established for the systems of records, pursuant to 5 U.S.C. 552a(b)(3), (e)(4)(D), and (e)(11). It should be noted that most DoD Components have published routine uses for personal records systems which print this disclosure. Likewise, the routine use provisions of the Office of Personnel Management System Notice for "General Personnel Records OPM/G0VT-1" published 25 November 1980 (44 FR 78415), contain the following statement, "d. To disclose information to: the Department of Labor; Veterans Administration, Social Security Administration; Department of Defense; Federal agencies that have special civilian employee retirement programs; or a national, state, county, municipal, or other publicly recognized charitable or Social Security Administration Agency (e.g., State unemployment compensation agencies),...." Therefore, the required information may be released.

14. RELEASE OF INFORMATION FOR PURPOSES OF COMMERCIAL SOLICITATION

The question presented is whether names and addresses of active duty, reserve or retired servicemembers may be withheld from disclosure under the Freedom of Information Act where the requester's primary purpose in seeking the information is to use it for commercial solicitation of those servicemembers. DOD information security policy prohibits the disclosure of names and duty addresses of servicemembers to any requester when such disclosure would reveal classified unit strengths or locations. *See* 5 U.S.C. §552 (b)(1); DOD 5400.7-R, paragraph 3-200, no. 1. However, unclassified name and address information about active duty, reserve or retired servicemembers may be released when its disclosure does not constitute a "clearly unwarranted invasion of personal privacy." 5 U.S.C. §552(b)(6).

In applying Exemption 6, the releasing authority must weigh the public interest in disclosure against the invasion of personal privacy that may result from the disclosure. *See Washington Post Co. v. Department of State,*

U.S._102 S. Ct. 1957, 1959-60 (1982) ("Congress primary purpose in enacting Exemption 6 was to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information"). The proper balance of the public interest against individual privacy requires the consideration of the stated or ascertained purpose of the particular requester. *See* DOD 5400.7-R, paragraph 3-200, no. 6b. The requester's interest in the agency records must reflect a purpose which would sufficiently further the public interest to justify any invasion of personal privacy.

A requester whose primary purpose for requesting servicemember's names and addresses is commercial solicitation normally should not be viewed as acting in the public interest. *See e.g., Wine Hobby USA, Inc. v. IRS,* 502 F.2d 133 (3d Cir. 1974); *HMG Marketing Associates v. Freeman,* 523 F. Supp. 11 (S.D.N.Y. 1980). Furthermore, where a requester seeks the home address or duty address of a servicemember primarily for commercial solicitation purposes, disclosure of that information necessarily involves at least some degree of invasion of personal privacy. As the Supreme Court has observed:

Today's merchandising methods the plethora of mass mailings subsidized by low postal rates and the growth of the sale of large mailing lists as an industry in itself have changed the mailman from, a carrier of primarily private ...communications and have made him an adjunct of the mass mailer who sends unsolicited and often unwanted mail into every home. It places no strain on the doctrine of judicial notice to observe that whether measured by pieces or pounds, Everyman's mail today is made up overwhelmingly of material he did not seek from persons he does not know. And all too often it is matter he finds offensive.

Rowan v. United States Post Office, 397 U.S. 728, 736 (1970). Therefore, in a situation where a requester has not established any public interest in obtaining service member's names and addresses, the invasion of privacy which would result from such disclosure requires that this information be withheld under Exemption 6's balancing test. In the rare case where a requester does establish some public interest involving his or her intention to engage in commercial solicitation, that interest must be weighed against any invasion of privacy which will result from disclosure of the requested information.

In sum, as the court observed in Wine Hobby, "[t]he disclosure of names of potential customers for commercial business is wholly unrelated to the purposes behind the Freedom of Information Act and was never contemplated by Congress in enacting the Act." 502 F.2d at 137. Therefore, neither a servicemember's home address nor a servicemember's duty address ordinarily should be provided to a FOIA requester whose primary purpose for seeking that information is commercial solicitation. This policy applies to active duty, reserve or retired personnel. Requesters who decline to indicate the purpose of their request for information concerning names and addresses should not be provided that information. DoD Components also should consider obtaining a notarized affidavit from requesters which indicates their purpose for requesting name and address information when those individuals have misrepresented their purpose for seeking information under past similar FOIA requests.

Disclosure of addresses of DoD civilian employees is governed by Office of Personnel Management regulations.

15. RELEASE OF INFORMATION CONTAINED IN MILITARY PERSONNEL RECORDS

The question presented is what information from personnel records is releasable to the public from military personnel records.

The criteria for the third party release of all personal information except that in investigative files is found in Exemption 6 of the Freedom of Information Act (5 U.S.C. 552(b)(6)). This exemption protects information the release of which would "constitute a clearly unwarranted invasion of personal privacy." The law indicates that a balancing test should be applied in releasing information under this standard and that the language "clearly unwarranted" tilts the balance in favor of disclosure. (*See e.g. Air Force v. Rose,* 425 U.S. 352 (1976); *Board of Trade v. Commodity Futures Trading Commission,* 627 F.2d 329 (D.C. Cir., 1980); *Ditlow v. Schultz,* 517 F.2d 166 (D.C. Cir., 1975)). The privacy invasion must be tangible and substantial. "... Exemption 6 was directed at threats to privacy interest, more palpable than mere possibilities." *Rose, supra* at 380, n. 19.

In applying Exemption 6, the releasing authority must weigh the public interest in disclosure against the invasion of personal privacy that will result from the disclosure. The proper balance of the public interest against individual privacy requires the consideration of the stated or ascertained purpose of the particular requester. DoD 5400.7-R, paragraph 3-200, no. 6b. The requester's interest in the agency records must reflect a purpose which, would sufficiently further the public interest to justify the incursion on personal privacy.

Although it is not possible to categorically identify information that must be withheld or released from military records in every instance, the following items of personal information may normally be released from military records without an unwarranted invasion of personal privacy; name, rank, date of rank, gross salary, present and past duty assignments, future assignments which have been finalized, duty or office telephone number, source of commission, military and civilian educational level, and promotion sequence number.

In addition, whenever a requester's interest can be adequately served by obtaining information that is not linked to a specific person, a denial authority may provide such information after deleting names, personal identifiers and other identifying information of individuals other than the requester. There is substantial support for this approach. *See e.g., Rose, supra* at 578-82; *National Prison Project of ACLU Foundation v. Sigler,* 390 F. Supp. 789,794 (D.D.C., 1975); 5 U.S.C. §552(a)(2).

The release of personal information to third parties from qualifying investigative files should be made using Exemption 7(C) (5 U.S.C. 552(b)(7)(C)). This exemption provides for the protection of information which would "constitute an unwarranted invasion of personal privacy."

The absence of the word "clearly" from the subsection makes this standard less tilted toward disclosure. Thus while a balancing test is required, the releasing authority should generally give more emphasis to the reasons to withhold than when using the Exemption 6 test discussed above.

Note. When releasing information about civilian employees, see the *Federal Personnel Manual.*

16. PROVIDING INFORMATION ON FEDERAL EMPLOYEES AND MILITARY MEMBERS TO FINANCIAL INSTITUTIONS

What information may be provided concerning Federal employees and military members in response to a credit investigation inquiry by a credit bureau or other representative of the credit granting industry?

Subparagraph B.2. of enclosure 5 of DoD Directive 5400.11 of August 4, 1975, Subj.: Personal Privacy and Rights of Individuals Regarding Their Personal Records, provides that information concerning a military member's rank, date of rank, salary, present and past duty assignments, future assignments which have been finalized, office phone number, and office address may be provided to any member of the public pursuant to the Freedom of Information Act (5 U.S.C. 552) and subsection (b)(2) of the Privacy Act. This information as well as other similar information such as the member's length of military service and duty status may be provided by any DoD activity unless the information has been classified in the interest of national defense or foreign policy.

It is further noted in this regard that subchapter 7 of chapter 294 of the *Federal Personnel Manual* authorizes the release of information concerning a Federal civilian employee's present and past position titles, grades, salaries, and duty stations (including office address) to the public if the information is not classified and is not being sought for political or commercial solicitation purposes. The cited subchapter further provides that credit firms may be provided more detailed information concerning tenure of employment, Civil Service status, length of service in the agency and the Federal Government, and certain information concerning the separation of an employee. It is considered that the Federal Personnel Manual provisions are consistent with the provisions of the Privacy Act and Freedom of Information Act in this regard.

Where the release of particular information requested by a credit bureau would not be authorized under the provisions described above, any personal information may be disclosed from military or civilian personnel records by DoD Components.. pursuant to subsection (b) of the Privacy Act, when there is written consent of the subject employee or military member specifically authorizing the release of the requested information.

See also a notice concerning Military Banking Facilities in the Federal Register of 13 February 1976 (41 FR 6779).

17. DISCLOSURE OF PHOTOGRAPHS IN THE CUSTODY OF THE DEPARTMENT OF DEFENSE

The question presented is whether official photographs in the custody of the Department of Defense may be released to the public and if a Privacy Act advice must be given when a photograph is taken. Photographs taken for official purposes of members of the armed forces and DoD employees are generally releasable under the Freedom of Information Act, 5 U.S.C. 552a(b)(2) unless the photograph depicts matters that if disclosed to public view would constitute a clearly unwarranted invasion of personal privacy. Generally, award ceremony photographs, selection file photographs, chain of command photographs and similar photographs are releasable. When such photographs are taken, it is not the collection of information contemplated by section (e)(3) of the Privacy Act and no Privacy Act advice is required.

18. DISCLOSURE OF RECORDS FROM SYSTEMS OF RECORDS TO A CONTRACTOR PURSUANT TO A CONTRACT

The question presented is whether disclosure of, personal records from a system of records to a contractor for the performance of a contract may be disclosed under section (b)(1) of the Privacy Act. The disclosure of records from systems of records to a contractor pursuant to sections 3(b)(1) and 3(m) of the Privacy Act requires neither, consent of the individual nor maintenance of a disclosure accounting record.

Section 3(m) of the Privacy Act, as interpreted by the Office of Management and Budget implementation guidelines (Federal Register, Volume 40, Number 132, pages 28975-2897 6) sets forth the necessary guidance in this matter. It provides that a system of records operated under contract to accomplish an agency function, is in effect deemed to be maintained by the agency. Under these guidelines, disclosures of personal information between an agency and its contractors fall under subsection 3(b)(1) of the Act, i.e., "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." The Privacy Act does not

impede disclosure of information to a contractor and system notices do not require any change to reflect use by a contractor.

19. APPLICATION OF LAW ENFORCEMENT PROVISIONS TO STATE AND LOCAL PROBATION, PAROLE OFFICERS, PENAL, MENTAL, AND/OR CORRECTIONAL INSTITUTIONS UNDER THE PRIVACY ACT

The question presented is whether state and local penal, mental and correctional institutions as well as probation and parole officers are law enforcement agencies within the provisions of the Privacy Act. Criminal law enforcement agencies and criminal justice means any activity pertaining to crime prevention control or reduction or the enforcement of the criminal law. Including. but not limited to, police efforts to prevent, control, or reduce crime or to apprehend criminals, activities of courts having criminal jurisdictions and related agencies (including prosecutorial and defender service), activities of correctional, probation, or parole authorities, and programs relating to the prevention, control, or reduction of juvenile delinquency or narcotic addiction.

Criminal law enforcement agencies are those local, state, or federal agencies thereof, such as those described above, including probation officers, which perform the administration of criminal justice pursuant to lawful authority.

20. FORMAT FOR PRIVACY ACT STATEMENTS

The question presented is what format should be followed in printing Privacy Act statements. The placements of the Privacy Act statement in a form should be in the following order of precedence:

1. Enclosed in the body of the form, preferably below the title and positioned in such a manner that the individual will be advised of the information required by the Act, or a statement showing the location of this information before he begins to furnish any of the information requested.
2. Placed on the reverse of the form with an appropriate notation under the title of its location.
3. Attached to the form as a tear-off sheet.
4. Issued as a separate supplement to the form.

21. PRIVACY ACT STATEMENTS FOR INSPECTOR GENERAL COMPLAINT FORMS

The question presented is whether or not a Privacy Act advice (5 U.S.C. 552a(e)(3)) is required for Inspector General Complaint forms. This question arises because the Component does not initiate a request for information from the individual, but only asks for certain information in order to respond to a complaint which was voluntarily initiated by the individual himself. The initiation of a course of action by the voluntary action of an individual does not preclude the need for a Privacy Act statement. The purpose of providing a Privacy Act statement is the notion of informed consent since an individual should be provided with sufficient information about the request for information so he may make an informed decision as to whether or not to respond. See OMB Guidelines, (40 FR 28961), dated July 9, 1975. The intent of the Privacy Act is to, in all instances, advise individuals whenever they are requested to provide personal information as to the authority for collection of the information, the uses to be made of the information, whether it is voluntary or mandatory to provide the information, and the consequences of not providing the information. Whenever a Component asks for information, a Privacy Act statement must be provided. We perceive no difference between an Inspector General complaint which triggers a request for information and medical forms which are completed only after the individual voluntarily initiates a request for treatment. It has been determined by all agencies that all medical forms require a Privacy Act advice.

22. RECRUITMENT ADVERTISEMENTS IN THE PUBLIC MEDIA

The question presented is whether recruitment advertisements in newspapers, etc., requires the publishing of a Privacy Act statement if a mail in coupon is provided for those individuals who desire further information.

Insofar as the published coupons and business return postcards merely provide the individual a vehicle with which he can request information from the military service concerning a particular recruiting program, no Privacy Act statement is required, as the service has not solicited information from the individual up to that point. The coupon or postcard used as a vehicle for the individual's solicitation of the service could include blanks for the individual's name address phone number and other blocks for the individual to indicate. His interest in a particular program and/or to provide information regarding his or her eligibility for a particular program (i.e., age, education level and sex). The individual's SSN does not appear to serve a significant purpose in the process of providing appropriate information to interested persons. If it is necessary for internal accounting purposes to include a blank for the individual's SSN, then a Privacy Act statement similar, to the one below would be sufficient if it reflects the uses to be made of the SSN.

"We will be happy to provide you more information about the Army opportunities as authorized by 10 U.S.C. 503. The

information voluntarily submitted, including your social security number, will be used for recruiting purpose. Failure to provide sufficient information may preclude action on your inquiry."

23. REQUIREMENT FOR PRIVACY ACT STATEMENT WHEN INFORMATION REQUESTED IS IN PUBLIC DOMAIN

The question presented is whether the Privacy Act advice specified under section (e)(3) of the act must be given when the only information sought must be disclosed under the FOIA. Paragraph B, enclosure 6, DoD Directive 5400.11 requires that Privacy Act advice be given whenever an individual is requested to supply personal information. The Privacy Act requirement, 5 U.S.C. 552a(e)(3), is not necessary when the only information requested is that which is required to be disclosed by the FOIA, providing the disclosure of such information does not inferentially disclose other personal information not releasable under the FOIA. Examples of such information are, but not limited to, name, grade, organization, duty assignment, and official telephone number.

24. IMPLICATIONS ON VARIOUS MODES OF RELEASING LEAVE AND EARNING STATEMENTS

The question presented is the distribution of leave and earning statements (LES) in consideration of good management practices, cost effectiveness, and the requirements of the Privacy Act.

There are basically three modes of distribution within the DOD: (1) the LES is mailed to the individual's home address. (2) The LES is handed out by office clerical personnel either with or without the pay check; or (3) the LES is handed out in an envelope by office clerical personnel with or without the pay check.

Leave and earning statements do contain personal information which is protected by the Privacy Act. Distribution may be made in any manner so long as the information is not disclosed to persons other than those that have a requirement to process the statements in the course of their official duties. Hence, any of the modes presented would be acceptable under the Privacy Act if the procedures preclude unauthorized disclosure to individuals outside the leave and earnings system.

25. THE APPEARANCE OF SOCIAL SECURITY NUMBER IN WINDOW OF ENVELOPES CONTAINING PERSONAL DOCUMENTS DOES NOT CONSTITUTE A DISCLOSURE

The appearance of Social Security Numbers in window envelopes does not constitute a "disclosure" as contemplated by the Privacy Act. Prior to delivery to the recipient, the only likely disclosure is the personnel of the postal service as agents who handle the letter in the performance of their official duties under agreement with the Department of Defense. However, consideration should be given when revising formats of the document or envelope to eliminate the appearance of the Social Security Number through the window of the envelope.

26. WHAT CONSTITUTES A PRIVACY ACT REQUEST FOR ACCESS OR AMENDMENT FOR THE PURPOSE OF COMPLIANCE WITH PROCESSING AND REPORTING REQUIREMENT?

There is no requirement in the Privacy Act that a request specify or cite that law before it is to be processed or accounted for as a Privacy Act request. As a matter of policy it is recommended that only requests which specify or clearly imply that they are being made under the Privacy Act receive the processing required by the law and implementing regulations and be reported as "Privacy Act requests." This would avoid inclusion of routine record checks and requests to modify or update data elements in record systems.

27. A PARENT OR GUARDIAN MAY HAVE ACCESS TO MEDICAL DETERMINATIONS FROM A MINOR'S MEDICAL FILE

In accordance with the definition of an "individual", contained in DoD Directive 5400.11, dated August 4, 1975, a legal guardian or the parent of a minor has the same rights as the individual and may act on behalf of the individual. The question presented is at what age is a dependent considered a minor for parental or guardian access to medical records under the Privacy Act. This must be determined on an individual basis by the state law governing the situs of the medical facility where the records are maintained. Although a determination may be made that the individual concerned is a minor under state law, and the information releasable to a parent or guardian, various state laws afford protection to certain types of medical records about individuals, e.g., drug abuse treatment, abortion, birth control devices, etc. This type of information should not be released if the state law prohibits release. This determination is not intended to suggest that minors are precluded from exercising rights on their own behalf. Except as otherwise provided in DoD Directive 5400.11, a minor does have the right to access a medical record pertaining to him or herself.

28. THIRD PARTY PERSONAL INFORMATION MAY BE PROTECTED BY THE ACT

The question presented is the extent to which third parties are protected by the Privacy Act against disclosure of personal information concerning them that may be contained in records of other individuals which are properly releasable to such individuals pursuant to the Act.

The question of third party privacy is not addressed directly in the Act. However, it is to be assumed that considerations of third party privacy have a bearing on the decision to release records pursuant to a Privacy Act request. The Privacy Act recognizes that one's "record," by definition, only contains information about that individual, the subject of the record. Furthermore, the Privacy Act provides that any information in a system of records "pertaining to" the subject of the record must be released (with certain exceptions not here germane). A record or portion thereof "pertains" to the subject of the record when the information is relevant to and is or was used in determining the subject's entitlement to rights, benefits, or privileges. For example, personal data such as SSNs and home addresses of third parties normally under these criteria do not "pertain" to the subject and need not be released, but information about the relationship between the subject and the third party would normally be disclosed as "pertaining" to the subject.

DoD Components maintaining a cross-indexed "system of records" should release information located in one's Privacy Act "record" only if the requested information pertains to the requester. Therefore, if an investigation of Subject A results in information about Subject B being placed in Subject A's investigators file and this file is indexed under both Subject A's and Subject B's name or personal identifier. Subject B may only obtain access under the Privacy Act to information pertaining to him or her. Subject B may not obtain access to information pertaining solely to Subject A.

29. REQUESTS FOR HOME ADDRESSES OF DOD PERSONNEL WHO STAND TO BENEFIT FROM THE RELEASE

Normally the release of home addresses and home telephone numbers of current or former service members would constitute a "clearly unwarranted invasion of personal privacy." However, when considering such a release, either under the strictures of the Privacy Act or the Freedom of Information Act, one must always balance the benefits of release against the privacy rights of the affected individuals. Further matters of appropriate consideration are the severity of the invasion of privacy, whether an invasion occurs at all, and the public purpose sought to be served by the requestor. When the requestor certifies in writing that his sole purpose in requesting the information is to enable him to confer a benefit upon an individual, such a disclosure would not rise to the level of a "clearly unwarranted invasion of personal privacy", and therefore should be permitted. This rationale holds true whether the release of home address is from systems of records subject to the Privacy Act or from records in general. Under the Privacy Act a nonconsensual release from a system of records subject to the Act is permissible where the release would be required under the Freedom of Information Act. Therefore. under the sixth exemption to the Freedom of Information Act, release of home addresses would only be prohibited where the release would constitute a "clearly unwarranted invasion of personal privacy." In the case where a benefit is sought to be conferred by the requestor the release would not rise to the level of a "clearly unwarranted invasion of personal privacy."

30. DISCLOSURE OF SECURITY CLEARANCE LEVEL

If the information as to an individual's Security Clearance is classified, it is protected from disclosure under the Privacy Act, 5 U.S.C. 552a(k)(1). If it is unclassified, the determination as to disclosure must be made under the Freedom of Information Act, 5 U.S.C. 552(b)(6). The determination would have to be made using the balancing test, balancing the public's; right to know against the individual's right of privacy. See *Department of the Air Force v. Rose,* 96 SCt 1592 (1976).

31. APPLICABILITY TO LEGAL MEMORANDA MAINTAINED IN A SYSTEM OF RECORDS

The question presented is whether an attorney's "work product" maintained in a system of records which pertains to a person must be disclosed to that person upon request under the Privacy Act. This determination does not apply to that work product which is not maintained in a "system of records" retrievable by name or identifying number.

Section (d)(5) of the Privacy Act specifically denies authority for individuals to have access to any information compiled in reasonable anticipation of a civil action or proceeding. Therefore, not only is an attorney's "work product" protected from access but other information which is not routinely released but is "compiled" in reasonable anticipation of litigation is protected. Once "work product" is prepared in reasonable anticipation of litigation, section (d)(5) would continue to protect the material regardless of whether litigation is instituted, completed or dropped.

The determination as to whether material is prepared in anticipation of litigation must be made on an ad hoe basis for each document in question. In making this determination, all circumstances must be considered including the intent of the author at the time the document was prepared.

32. FILES INDEXED BY NON-PERSONAL IDENTIFIER CONTAINING PERSONAL INFORMATION RETRIEVABLE BY MEMORY, AS OPPOSED TO ANY INDEX KEYED TO PERSONAL IDENTIFIERS, DOES NOT FALL UNDER THE CRITERIA OF THE ACT

The labeling of files by non-personal identifiers makes the access requirements of the Privacy Act inapplicable, unless such files are in fact retrieved on the basis of an individual identifier through a cross-reference system or some other

medium or method. The human memory alone does not constitute a cross-reference system and consequently is not a criteria.

33. COMPUTER CARDS AND PRINTOUTS NEED NOT BE DEPERSONALIZED BEFORE DISPOSAL

A massive release for disposal of computer cards and printouts is not a disclosure of personal information which would be precluded by the Privacy Act. In view of the volume of the "records" and the coding of information it is impossible to pinpoint any comprehensive information about a specific individual. Therefore such computer products may be turned over to Defense Property Disposal offices for disposal, sale as scrap, or recycling, as appropriate, as was done prior to the enactment of the Privacy Act, without deleting the names or other individual identifying data.

34. SUPPLEMENTAL CHARGES MAY NOT BE ASSESSED FOR UNLISTED TELEPHONE NUMBER SERVICES TO MILITARY AND CIVILIAN PERSONNEL (CLASS B SUBSCRIBERS) WHO LIVE ON INSTALLATIONS WHERE NO COMMERCIAL SERVICE IS AVAILABLE

An individual should have the opportunity to elect not to have his home address and telephone number listed in a base telephone directory. He is excused from paying for the additional cost that may be involved in maintaining an unlisted number if he complies with the regulations providing for such unlisted numbers.

35. THE (j)(2) GENERAL EXEMPTION DOES NOT FOLLOW THE RECORD

A record created and maintained in a law enforcement system of records and properly exempted under section (j)(2) of the Privacy Act may not retain the (j)(2) exemption when a copy thereof is permanently included in a system of records maintained by a non-law enforcement activity. Specifically, copies of records, which would otherwise be afforded a general exemption will lose their exempt character when permanently filed in nonexempt systems.

Invoking the (j)(2) general exemption should be limited to certain systems of records maintained only by DoD investigative activities, i.e., USAINTA, USCIDC, NIS, AFOSI, Military Police, etc., which perform as their principal function any activity pertaining to the enforcement of criminal laws and not to systems of records maintained by any other DoD activity that may have copies of reports of investigations. It is the intent of Congress that only activities, which perform law enforcement functions are entitled to this general exemption for a record system. The permanent filing of law enforcement records exempted under section (j)(2) in another records system will not permit a non-law enforcement activity to invoke and claim the (j)(2) exemption for that entire system of records merely because a few law enforcement files are maintained therein.

Individuals seeking access under the Privacy Act to investigate records in the temporary custody of an element shall be directed to the originating investigative organization. However, records concerning adjudication, or other personnel actions based on law enforcement records, originated by the element using the investigation, are the records, without the (j)(2) exemption, of the using element which shall respond to all other requests under the Privacy Act concerning them.

36. THE SYSTEM NOTICE REQUIREMENT UNDER THE PRIVACY ACT APPLIES TO COURT-MARTIAL FILES

Records of courts-martial trials, unless classified, have always been considered public records and are released upon request to the public. The procedures and policies regarding courts-martial are governed by the UCMJ and the Manual for courts-martial (MCM) 1969 (Revised). Congress recognized the unique nature of courts-martial proceedings and exempted them from the requirements of the Administrative Procedure Act by specifically excluding them from the definition of "agency" (5 U.S.C. 551 (1)(F)). Although courts-martial are not "agencies" by definition and Section 2(b), the preamble to the Privacy Act, states: "The purpose of this Act is to provide certain safeguards ... by requiring Federal agencies, except as otherwise provided by law, to...", section (c)(4) of the Privacy Act requires each agency that maintains a system of records to "publish in the Federal Register at least annually a notice of the existence and description of the system of records." The requirement to publish a system notice applies to systems containing courts-martial records since the "record" of the proceeding is maintained by an agency long after the courts-martial involved has been dissolved. All agencies maintaining such records should publish a system notice pertaining to courts-martial records of trial.

37. A GENERAL ROUTINE USE FOR DISCLOSURE TO THE NATIONAL ARCHIVES AND RECORDS CENTER, GSA, APPLICABLE TO DOD RECORDS, IS NOT REQUIRED

The Federal Records Act of 1950, as implemented by the Federal Property Management Regulations, does not require a general Department of Defense routine use notice for DoD records systems. A DoD "boiler-plate" routine use for disclosure to the National Archives and Records Service, General Services Administration (GSA) is not deemed necessary.

Disclosure to the National Archives of documents which warrant continued preservation is authorized by section

(3)(b)(6), 5 U.S.C. 552a, the Privacy Act of 1974. The transfer of DoD Component records to GSA for storage does not alter "ownership" of the records; however, employees of GSA are agents of the Components when inspecting and processing these stored records and therefore disclosure to them is authorized under section (b)(1) of the Act as they are properly considered employees of the Component when performing these duties.

The Privacy Act was not intended to supersede other Federal statutes which require disclosure of records containing personal information. The statement of purpose contained hl section 2(b), the preamble to the Privacy Act, states: "The purpose of this Act is to provide certain safeguards . . ., except as provided by law, to..." Further, 44 U.S.C. 2906 specifically authorized and requires disclosure of records in custody of agencies to GSA employees so they may inspect and survey such records.

38. DEFINITION OF "ORDER OF A COURT OF COMPETENT JURISDICTION" UNDER 5 U.S.C. 552a(b)(11)

A subpoena signed by a clerk of a Federal or State court does not comprise an "order of a court of competent jurisdiction" for purposes of subsection (b)(11) of the Privacy Act, 5 U.S.C. 552a. An "order of a court of competent jurisdiction" for purposes of subsection 5 U.S.C. 552a(b)(11) must be signed by a State or Federal court judge. Although the Privacy Act and its legislative history offer no definition of the term "court order," a court order may be defined in general as a directive issued under judicial authority and subject to enforcement in a court of law. Thus, for the purposes of subsection (b)(11) of the Privacy Act, an order of a court of competent jurisdiction includes any order or writ issued by a Federal or State judge in aid of his or her jurisdiction, ordering the production of records, which is issued under authority of Federal or State law or rules of court and which is enforceable by judicial process.

39. SERVICE ORIENTED SOCIAL WELFARE ORGANIZATION MAY BE LISTED AND GRANTED ACCESS TO PERSONNEL AND PAY RECORDS AS A ROUTINE USER

The disclosure of personal information from record systems, such as personnel and pay, to service oriented social welfare organizations, e.g., Army Emergency Relief, Navy Relief, Air Force Aid Society, American Red Cross, USO, etc., properly established as routine users, is permissible under the Privacy Act. However, only such information as is necessary for the welfare agency to perform its authorized functions should be provided. The information can be disclosed only if the agency ,which receives it adequately prevents its disclosure to persons other than their employees who need such information to perform their authorized duties.

40. PRIVACY ACT WARNING LABELS

The use of Privacy Act Warning Labels should be left optional to the discretion of each DoD Component. This includes any new Civil Service Commission Personal Data Warning Labels (Optional Forms 86 and 86-A). The use is optional, but DoD Components are under an obligation under subsection 3(e)(10) of the Privacy Act to establish appropriate safeguards for personal information. No particular existing warning label produced within or outside of the DoD appears to be entirely satisfactory and acceptable for adoption and uniform application to all DoD Components. Therefore, each DoD Component may at their discretion independently design or adopt existing labels and prescribe their internal use.

41. FURNISHING LISTS OF PERSONNEL RESIDING IN GOVERNMENT QUARTERS TO LOCAL GOVERNMENTS FOR TAX PURPOSES

A request by local, county or city governments for a list of the persons occupying US Government quarters for the purpose of possible enforcement and collection of local taxes is permissible. Disclosure of the list of occupants could not be considered a clearly unwarranted invasion of privacy and would be required under the Freedom of Information Act for the same rationale as the IRS Form W-2 information is supplied to state taxing authorities. Moreover, there is an established general routine use published by all DoD Components concerning disclosure to state and local taxing authorities.

42. DISCLOSURE OF PERSONAL INFORMATION CONCERNING SAVINGS BONDS PROGRAM PARTICIPANTS

Access to information contained in systems of records concerning employee participation in the Savings Bond Program may be necessary to those officers and employees of the DoD Components maintaining the systems of records who have a need for the record in the performance of their duties, (5 U.S.C. 552a(b)(1)). Disclosure under the (b)(1) provision is based on a "need-to-know" concept. Consequently while disclosure to those personnel who require access to the records to discharge their duties such as payroll and allotment clerks, key men and campaign aides who assist directly in the implementation of the program would be authorized. The disclosure to supervisors is neither directly related to any campaign program requirement nor consistent with the disclosure provisions of the Privacy Act. Disclosure should be restricted to only those personnel with a direct functional relationship to a campaign and for

campaign purposes only. Personnel who are authorized to receive this information should be briefed on their responsibilities under the Act and warned against unauthorized disclosure.

43. PERSONAL NOTES OR RECORDS

The personal handwritten notes of unit leaders or office supervisors concerning subordinates are not systems of records maintained by the government as contemplated by the Privacy Act. Such notes are an extension of the individual's memory rather than the "memory" of an agency, and may be used solely to refresh the individual's memory. The notes, however, must be maintained and discarded at the sole discretion of the individual generating such notes. Any requirement by superior authority to maintain such notes, e.g., written or oral directive, regulation, or command policy, would cause the notes to become "agency records" and thus subject them to the Privacy Act. Furthermore, actions which give these notes the appearance of agency records rather than personal notes, such as passing them to a successor, would necessitate their incorporation into a system of records that is subject to the Act.

Individuals who maintain such notes must restrict their use exclusively to that of a memory aid. Personal notes should not be used in lieu of official personnel files when making personnel determinations affecting subordinates. Furthermore, extreme caution should be exercised when making disclosures from personal notes or when discarding such notes. Disclosures from personal notes, either intentional or through careless protection or disposal may subject the individual or the agency to litigation if such disclosures would not be permitted by the Act. Individuals maintaining these notes are subject to the Act, even though such notes themselves, are not. Therefore they are accountable for disclosures from their personal notes to the same degree that they are accountable for disclosures of personal information obtained in the performance of their duties and disclosed from memory.

44. PRIVACY ACT STATEMENT REQUIREMENTS TO THIRD PARTIES IN CONNECTION WITH ADMINISTRATIVE PROCEEDINGS

The collection of personal information from an individual in an administrative proceeding, the record of which will be maintained in a system of records retrievable by the individual's name or some personal identifier, must be preceded by the provision of an appropriate Privacy Act Statement.

45. THE AGE OF MAJORITY IS 18 YEARS FOR PURPOSES OF PARENTAL ACCESS TO MEDICAL DETERMINATIONS FROM A MINOR'S MEDICAL FILES AT OVERSEAS INSTALLATIONS

The question is at what age is a dependent considered a minor for parental or guardian access to medical records under the Privacy Act at overseas installation. The problem arises due to the absence of relevant state laws at such installations, as well as the impracticability of reliance upon home of record. For purposes of implementation of the relevant Privacy Act provisions at overseas installations, therefore, reliance should be placed upon the vast weight of authority with establishes 18 years as the age of majority.

46. ACCESS TO MEDICAL RECORDS BY THIRD PERSONS DESIGNATED BY THE RECORD SUBJECT

A medical record shall be disclosed to the individual to whom it pertains unless a judgment is made that access to such records could have an adverse effect upon the individual's physical or mental health. Normally this judgment should be made in consultation with a medical doctor.

When it is determined that the disclosure of medical information could have an adverse effect upon the individual to whom it pertains, the information should be transmitted to a physician named by the requesting individual and not directly to the individual. However, the physician should not be required to request the record on behalf of the individual. Information which may be harmful to the record subject should not be released to a designated individual unless the designee is qualified to make psychiatric or medical determinations. If the individual refuses to provide a qualified designee, the request for the medical records should not be honored.

47. DOD COMPONENTS ARE NOT RESPONSIBLE FOR THE REPRODUCTION AND AVAILABILITY OF ANY PRIVACY ACT STATEMENTS FOR USE BY LABOR ORGANIZATIONS

It is not a violation of the Privacy Act for the labor organization to provide personal information obtained from one of the members to a DoD Component for the purpose of facilitating the allotment of union dues, even though the employee-union member, is not given a Privacy Act Statement when he volunteers the information to the labor organization.

The Privacy Act of 1974 does not apply to labor organizations. Labor organizations are not required under the Act to give Privacy Act Statements to U.S. Government employees before obtaining personal information for a voluntary allotment of union dues. Any use of the Privacy Act Statement by a labor organization is voluntary, and may result from express agreement with a DoD Component or as a spontaneous union practice.

Under E. O. 11491, as amended, labor organizations occupy a unique relationship with U.S. Government agencies. The

Civil Service Commission currently requires that a labor organization use a Standard Form 1187 to obtain personal information necessary for an allotment of union dues. Under these circumstances it would be consistent with the spirit of the Privacy Act to urge labor organizations to provide the Commission's Privacy Act Statement when using that form. To this end, a union and a DoD Component could agree that copies of the Commission Statement be provided to the union for its use.

48. SECURITY RESPONSIBILITY RECORDS CONTAINING PERSONAL INFORMATION ATTACHED TO SECURITY CONTAINERS OR FACILITIES REQUIRE PRIVACY ACT STATEMENTS AND PROTECTION FROM DISCLOSURE

Personal information consisting of name, home address, and telephone number of persons designated as custodians of security storage containers or facilities is protected by the Privacy Act. The solicitation of such information is justified as necessary to an appropriate routine use, but it requires issuance of a Privacy Act Statement without regard to whether the information is to be maintained in a system of records. This information, when appended to the exterior of a storage facility or container, is observable by any passer-by and is not necessarily limited to officers and employees officially concerned with the activity. Therefore, it is considered a disclosure subject to the disclosure accounting requirements to the Act. Such disclosure accounting, however, would be impossible because of the difficulty of identifying all viewers.

The General Services Administration (GSA) has recognized that this information is personal in nature and has revised Optional Form 63 to include a Privacy Act Statement and to instruct that the form be attached to the interiors of safes. Paragraph 5-104 of DoD Regulation 5200.1-R, "Information Security Program Regulation", permits the use of GSA Optional Form 63 (Rev. 10-75) within the DoD. When such a tag is placed inside a safe, the disclosure is limited to those officers and employees who have a need-to-know and no disclosure accounting is required.

Alternatives to the disclosure accounting requirements are: (1) to obtain the individual's prior written consent for a single particular transaction, i.e., consent to disclose name, home address, and telephone number for a particular safe or (2) to require notification of appropriate duty personnel with access to a control roster containing the custodian personal information that they be contacted in the case of a possible security problem.

49. VERIFICATION OR CERTIFICATION OF THE ACCURACY OF PERSONAL DATA ON A FORM OR RECORD IS SUBJECT TO PRIVACY ACT NOTIFICATION REQUIREMENTS

The act of verification or certification of the accuracy of personal data on a form or record constitutes the collection of personal data from an individual and is subject to the provisions of subsection (e)(3) of the Privacy Act. Guidance on the implementation of this subsection issued by the Office of Management and Budget supports this conclusion. Subsection (e)(3) is intended "to assure that individuals from whom information about themselves is collected are informed of the reasons for requesting the information, how it may be used, and what the consequences are, if any, of not providing (or failing to accurately provide) the information." (OMB Ltr., Subj.: Guidelines for Implementing Section 3 of the Privacy Act, dtd 1 July 1975, at 48-49.)

Any of these three situations would invoke the provisions of the Privacy Act. First, to verify a record requires the individual to examine and to disclose whether or not the record is correct. A request for verification from the individual is a request for personal information from the individual. The acknowledgement of the truthfulness of the underlying data is itself a personal disclosure. Second, the individual is asked to identify any erroneous entries and to *furnish* the correct data. When the request is soliciting corrections and additions to the subject records, any response is an outright disclosure of personal information. Third, a verification standing alone, equivalent to a certification, in effect, requests the individual to *republish* as truthful the underlying personal information. Any verification is adopting by reference the existing data as the verifier's own and thereby has the effect of republishing the basic information.

50. HEALTH CARE RECORDS OF A DOD COMPONENT MAY BE DISCLOSED TO ANOTHER DOD COMPONENT FOR VALID MEDICAL RESEARCH PROGRAMS WITHOUT INDIVIDUAL CONSENT OR A ROUTINE USE

The Department of Defense is considered a single agency for the purpose of disclosures within. A record in a system of records from one DoD Component may be disclosed, without the consent of the individual to whom the record pertains, if disclosure would be, pursuant to subsection 3(b)(1) of the Privacy Act, to those officers and employees of another DoD Component who have a need for the record in the performance of their duties and the use is compatible with the purpose for which the record is maintained. This permissive transfer of information between DoD Components does not require a published external routine use notice for the record system, and no disclosure accounting is required.

51. THE ORIGINAL SERIAL NUMBER (SERVICE NUMBER) ASSIGNED TO MILITARY PERSONNEL UNTIL REPLACED BY THE SOCIAL SECURITY NUMBER IN 1967 DOES NOT CONSTITUTE PERSONAL INFORMATION

The issue presented was whether the original serial number, later called the service number, which the military services assigned to military personnel up until 1967 when it was replaced by the Social Security Number (SSN), constituted personal information which should not be released to third parties.

It was determined that the old serial/service number did not have the same significance or importance as the SSN. The serial/service number, in and of itself, is no longer a personal identifier. It cannot be used to facilitate unconstrained linkage, consolidation, or exchange of information about an individual through multiple data banks in multifarious ways or at widespread locations even within DoD. Therefore, disclosure may be made of orders and similar documents which compromise listings of names and serial/service numbers without expunging such numbers, with no invasion of personal privacy.

The old serial/service number should not be confused with the SSN which can act as a key to unlock innumerable data bases and provide easy access to much personal information, both within and without the DoD.

52. THE USE OF THE SOCIAL SECURITY NUMBER ON BUILDING AND INSTALLATION BADGES IS A PERSONAL IDENTIFIER

A Social Security Number (SSN) on Defense Department building and identification badges required to be prominently displayed or worn at all times constitutes a personal identifier under the Privacy Act. The SSN, with an individual's name, is personal information and a personal identifier. This information when displayed on an exposed identification badge is observable by any passerby and is not necessarily limited to the officers and employees officially concerned with the intended use of the badge. It amounts to a constant verification from the individual who is certifying and republishing as truthful the basic personal information being advertised. Providing a Privacy Act Statement and maintaining disclosure accounting would be impossible because of the large and varying number of viewers.

Physical security should not be hampered with the omission of the SSN from such open display and consideration should be given to eliminate the SSN from such badges when issued or reissued on an attrition or replacement basis.

53. USE OF A (j)(2) AND (k)(2) EXEMPTION FOR THE SAME SYSTEM OF RECORDS

The (j)(2) and (k)(2) exemption cannot be used for the same system of records. The system of records must be a system of law enforcement records maintained by a law enforcement activity in order to qualify for the (j)(2) exemption. Only non-law enforcement activities, which retain law enforcement records in their system of records qualify for the (k)(2) exemption. Therefore, a single system of records should not be exempted under both exemptions. However, a single system of records maintained by a law enforcement activity may contain law enforcement records, which may be exempted under (j)(2) and personnel security records which are exempted under (k)(5). Where the two types of records are clearly segregable in a single system then the use of these two exemptions, (j)(2) and (k)(5), would appear acceptable. Also records systems may contain records which may be exempted under more than one provision of the (k) exemption. Only previously published exemptions established in accordance with DoD Directive 5400.11 may be used for any system of records.

54. RELEASE OF THIRD PARTY DATA PREVIOUSLY FURNISHED TO AN INDIVIDUAL FROM OFFICIAL PERSONNEL RECORDS

Prior to implementation of the Privacy Act in September 1975, some Components issued blanket orders or other official documentation concerning all or many affected personnel for such personnel actions as promotions, discharges, TDY, PCSs, etc. The release of these documents which contain limited amounts of third party personal data such as SSNs, homes of record, home address as of the date of the record, etc. to an individual is not a clearly unwarranted invasion of privacy and prohibited by the Privacy Act if:

1. The document concerns the requesting individual and is filed in his official personnel record,
2. The document was previously furnished to the requesting individual, and
3. The document was created prior to September 27, 1975.

Nothing in this decision should be construed as limiting the release to an individual of third party information which would normally be released under the provisions of the Freedom of Information Act (5 U.S.C. 552).

Index

USAPA

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER .WIN32 Version 1.09

PIN: 052882–000
DATE: 06-12-00
TIME: 10:53:49
PAGES SET: 22

DATA FILE: C:\wincomp\nich.fil
DOCUMENT: DA PAM 340–6
DOC STATUS: NEW PUBLICATION